Safeguarding Customer Financial Information

Safeguarding Customer Financial Information

Sec. 38a-8-124. Definitions

As used in sections 38a-8-124 to 38a-8-126, inclusive, of the Regulations of Connecticut State Agencies:

(1) ''Customer'' means ''customer'' as defined in section 38a-8-106 of the Regulations of Connecticut State Agencies.

(2) ''Customer information'' means ''nonpublic personal financial information'' as defined in section 38a-8-106 of the Regulations of Connecticut State Agencies, about a customer, whether in paper, electronic, or other form that is maintained by or on behalf of the licensee.

(3) ''Customer information systems'' means the methods used to access, collect, store, use, transmit, protect or dispose of customer information, and includes, but is not limited to, an ''information processing system'' as defined in section 1-267 of the Connecticut General Statutes.

(4) ''Licensee'' means ''licensee'' as defined in section 38a-8-106 of the Regulations of Connecticut State Agencies.

(5) ''Service provider'' means a person that provides services to the licensee and maintains, processes or otherwise is permitted access to customer information.

(Adopted effective January 1, 2004)

Sec. 38a-8-125. Information security program

Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the

protection of customer information that are appropriate to the size and complexity of the licensee and the nature and scope of its activities. Each information security program shall be designed to: ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of customer information; and protect against unauthorized access to, or use of, customer information that could result in substantial harm or inconvenience to any customer.

(Adopted effective January 1, 2004)

Sec. 38a-8-126. Developing and implementing an information security program

The actions and procedures described in this section are examples of methods of implementation of the requirements of section 38a-8-125 of the Regulations of Connecticut State Agencies. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement section 38a-8-125 of the Regulations of Connecticut State Agencies.

(1) The licensee identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems. The licensee assesses the likelihood and potential damage of the risks presented by the threats it has identified, taking into consideration the sensitivity of customer information. The licensee assesses the sufficiency of the policies and procedures it has in place to control the risks it has identified.

(2) The licensee designs its information security program to control the identified risks, commensurate with the sensitivity of the information and the complexity and scope of the licensee's activities. The licensee trains staff, as appropriate, to implement the licensee's information security program and regularly tests or otherwise regularly monitors the key controls, systems and procedures of its information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

(3) The licensee exercises due diligence in selecting service providers, and requires its service providers to implement measures designed to meet the objectives of section 38a-8-125 of the Regulations of Connecticut State Agencies and takes appropriate steps to confirm that its service providers have done so.

(4) The licensee monitors, evaluates and adjusts, as appropriate, its information security program to reflect any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to its customer information systems.

(Adopted effective January 1, 2004)